REMARKS

This is a full and timely response to the final Office Action of March 9, 2005. Upon entry of this Second Response, claims 1-24 are pending in this application. Reexamination, reconsideration, and allowance of the application and all presently pending claims are respectfully requested.

Interview Summary

Applicants wish to express their sincere appreciation for the time that Examiner Arani spent with Applicants' undersigned Agent and Attorney during a telephone discussion on April 21, 2005, regarding the outstanding Office Action. In the telephone conversation, no exhibits were discussed, and claim 20 was discussed with reference to *Pereira* (U.S. Patent No. 5,809,230). In this regard, Applicants' Agent and Attorney suggested that *Pereira* fails to disclose a "security setting" that is indicative of "whether access to (a) resource is restricted" and a "security application" that detects "an unauthorized change of said security setting" and automatically changes "said security setting... in response to a detection of an unauthorized change of said security setting," as described by claim 20.

In particular, *Pereira* appears to teach that an "access control program" is segmented into three components, and each component verifies that the other components are "loaded and are operational." See column 10, lines 48-67. Further, all three program components are apparently reloaded if any of the program components detects that the other program components have been changed. See column 11, lines 1-5. However, none of the program components appear to include a "security setting," as described by claim 20. In this regard, the program components appear to be executable computer code that uses various settings ***stored in external data files*** to protect the resources of a computer system. See column 9, lines 44-48. Thus, the detection of a modified

program component and subsequent reloading of the program component in *Pereira* does not constitute a detection of "an unauthorized change of said security setting" and a change of "said security setting... in response to a detection of an unauthorized change of said security setting," as described by claim 20. The Examiner seemed to agree and requested that Applicants submit a written response reflecting the same about the Office Action.

Response to §102 and §103 Rejections

A proper rejection of a claim under 35 U.S.C. §102 requires that a single prior art reference disclose each element of the claim. See, *e.g.*, *W.L. Gore & Assoc., Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303, 313 (Fed. Cir. 1983).

Claim 1

Claim 1 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Claim 1 presently reads as follows:

> 1. A computer system, comprising:
> memory; and
> a security application configured display a list of security rules to a user and to enable ones of said security rules based on user inputs, said security application configured to lock down resources of said computer system by modifying security settings of said computer system based on which of said security rules are enabled when an activation request is received by said computer system, said security application configured to store, in said memory, data indicative of said security settings, ***said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on one of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison***. (Emphasis added).

Applicants respectfully assert that the cited art fails to disclose at least the features of claim 1 highlighted hereinabove. Thus, the 35 U.S.C. §102 rejection of claim 1 is improper.

In this regard, it is asserted in the Office Action that *Pereira* teaches:

> "said security application configured to perform comparisons between said data and said security settings and to determine when one of said security settings has changed from a first value to another value based on once of said comparisons, said security application further configured to change said one security setting to said first value in response to said one comparison (column 10, lines 64-column 11, line 6)."

The cited section of *Pereira* appears to describe an "access control program" that restricts the use of resources within a computer system. However, for at least the reasons set forth above in the Interview Summary section, Applicants assert that "access control program" does not appear to include a "security setting." Thus, the cited section of *Pereira* fails to establish that at least the highlighted features of claim 1 are disclosed by *Pereira*.

For at least the above reasons, Applicants respectfully assert that *Pereira* fails to disclose each feature of claim 1. Accordingly, the 35 U.S.C. §102 rejection of claim 1 should be withdrawn.

Claims 2-4 and 11-17

Claim 2 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor* (U.S. Patent No. 6,530,024). Further claims 3, 4 and 11-17 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Applicants submit that the pending dependent claims 2-4 and 11-17 contain all features of their respective independent claim 1. Since claim 1 should be allowed, as argued hereinabove, pending dependent claims 2-4 and 11-17 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 5

Claim 5 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Claim 5 presently reads as follows:

> 5. A system for locking down resources of computer systems, comprising:
> means for receiving a request for activating a security profile;
> means for modifying security settings of a computer system in response to said request;
> means for storing data indicative of said modified security settings;
> ***means for automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and***
> ***means for automatically changing said one security setting to said first value in response to a determination by said determining means that said one security setting has changed***. (Emphasis added).

Applicants respectfully assert that the cited art fails to disclose at least the features of claim 5 highlighted hereinabove. Thus, the 35 U.S.C. §102 rejection of claim 5 is improper.

In this regard, it is asserted in the Office Action that *Pereira* teaches:

> "automatically determine when (one) of said security settings has changed from a first value to another by periodically comparing said data to said security settings (column 10, lines 64-column 11, line 3), automatically changing one security setting to said first value in response to a determination that one security setting has changed (column 11, lines 3-6)."

The cited sections of *Pereira* appear to describe an "access control program" that restricts the use of resources within a computer system. However, for at least the reasons set forth above in the Interview Summary section, Applicants assert that "access control program" does not appear to include a "security setting." Thus, the cited sections of *Pereira* fail to establish that at least the highlighted features of claim 5 are disclosed by *Pereira*.

For at least the above reasons, Applicants respectfully assert that *Pereira* fails to disclose each feature of claim 5. Accordingly, the 35 U.S.C. §102 rejection of claim 5 should be withdrawn.

Claims 6, 7, and 18

Claim 6 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor*. Further, claims 7 and 18 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Applicants submit that the pending dependent claims 6, 7, and 18 contain all features of their respective independent claim 5. Since claim 5 should be allowed, as argued hereinabove, pending dependent claims 6, 7, and 18 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 8

Claim 8 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Claim 8 presently reads as follows:

> 8. A method for locking down resources of computer systems, comprising:
> receiving a request for activating a security profile;
> modifying security settings of a computer system in response to said request;
> storing data indicative of said security settings, as modified by said modifying;
> ***automatically determining when one of said security settings has changed from a first value to another value by periodically comparing said data to said security settings; and***
> ***automatically changing said one security setting to said first value in response to a determination in said determining that said one security setting has changed***. (Emphasis added).

Applicants respectfully assert that the cited art fails to disclose at least the features of claim 8 highlighted hereinabove. Thus, the 35 U.S.C. §102 rejection of claim 8 is improper.

In this regard, it is asserted in the Office Action that *Pereira* teaches:

> "automatically determine when (one) of said security settings has changed from a first value to another by periodically comparing said data to said security settings (column 10, lines 64-column 11, line 3), automatically changing one security setting to said first value in response to a determination that one security setting has changed (column 11, lines 3-6)."

The cited sections of *Pereira* appear to describe an "access control program" that restricts the use of resources within a computer system. However, for at least the reasons set forth above in the Interview Summary section, Applicants assert that "access control program" does not appear to include a "security setting." Thus, the cited sections of *Pereira* fail to establish that at least the highlighted features of claim 8 are disclosed by *Pereira*.

For at least the above reasons, Applicants respectfully assert that *Pereira* fails to disclose each feature of claim 8. Accordingly, the 35 U.S.C. §102 rejection of claim 8 should be withdrawn.

Claims 9, 10, and 19

Claim 9 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor*. Further, claims 10 and 19 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Applicants submit that the pending dependent claims 9, 10, and 19 contain all features of their respective independent claim 8. Since claim 8 should be allowed, as argued hereinabove, pending dependent claims 9, 10, and 19 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

Claim 20

Claim 20 presently stands rejected under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Claim 20 presently reads as follows:

> 20. A computer system, comprising:
> memory;
> an operating system configured to analyze a machine state to control operation of said computer system, said machine state including a security setting associated with a resource of said computer system and indicating whether access to said resource is restricted, wherein said operating system is configured to analyze said security setting to control access to said resource; and
> a security application configured to modify said security setting based on a user input and to store, in said memory, data indicative of a state of said security setting, as modified by said security application, ***said security application configured to perform a comparison between said data and said security setting to detect an unauthorized change of said security setting, said security application further configured to automatically change said security setting based on said data in response to a detection of an unauthorized change of said security setting***. (Emphasis added).

For at least the reasons set forth hereinabove in Interview Summary section, Applicants respectfully submit that the cited art fails to disclose at least the features of claim 20 highlighted above. Accordingly, the 35 U.S.C. §102 rejection of claim 20 should be withdrawn.

Claims 21-24

Claims 21-23 presently stand rejected in the Office Action under 35 U.S.C. §102 as allegedly anticipated by *Pereira*. Further, claim 24 presently stands rejected in the Office Action under 35 U.S.C. §103 as purportedly unpatentable over *Pereira* in view of *Proctor*. Applicants submit that the pending dependent claims 21-24 contain all features of their respective independent claim 20. Since claim 20 should be allowed, as argued hereinabove, pending dependent claims 21-24 should be allowed as a matter of law for at least this reason. *In re Fine*, 5 U.S.P.Q.2d 1596, 1600 (Fed. Cir. 1988).

CONCLUSION

Applicants respectfully request that all outstanding objections and rejections be withdrawn and that this application and all presently pending claims be allowed to issue. If the Examiner has any questions or comments regarding Applicants' response, the Examiner is encouraged to telephone Applicants' undersigned counsel.

Respectfully submitted,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: 

Jon E. Holland
Reg. No. 41,077
(256) 704-3900 Ext. 103

Hewlett-Packard Development Company, L.P.
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400